Heuristics for the arithmetic of elliptic curves

Bjorn Poonen

(based on joint papers with Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra jr., Jennifer Park, Eric Rains, John Voight, and Melanie Matchett Wood)

August 4, 2018

Elliptic curves over $\mathbb{Q}$

Every elliptic curve E over $\mathbb{Q}$ is isomorphic to a unique one given by

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Z}$ satisfy $4A^3 + 27B^2 \neq 0$ and there is no prime p with $p^4|A$ and $p^6|B$.

- $\mathscr{E}$:= the set of such elliptic curves.
- $\operatorname{ht} E := \max(|4A^3|, |27B^2|)$ for each $E \in \mathscr{E}$.
- $\mathscr{E}_{\leq H} := \{E \in \mathscr{E} : \operatorname{ht} E \leq H\}$.

Proposition

$\#\mathscr{E}_{\leq H} \sim H^{5/6}$, *ignoring constants.*

Sketch of proof:
About $H^{1/3}$ choices for A, and about $H^{1/2}$ choices for B.

Rational points on elliptic curves

Theorem (Mordell 1922)

For each elliptic curve E over $\mathbb{Q}$,
the abelian group $E(\mathbb{Q})$ is finitely generated.

Thus $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ for some $r \geq 0$ and finite abelian group T.

Theorem (Mazur 1977)

The possibilities for the torsion subgroup T are

- $\mathbb{Z}/m\mathbb{Z}$ *for* $m \leq 12$ *excluding* 11, *and*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *for* $n \leq 4$.

What about the rank $r = \mathrm{rk}\, E(\mathbb{Q})$?

Is the rank bounded?

Poincaré 1901: What are the possibilities for the rank?

Implicit in Poincaré's question is the following:

Question

Is $\mathrm{rk}\, E(\mathbb{Q})$ *bounded as* E *varies over all elliptic curves over* $\mathbb{Q}$*?*

- Early authors conjectured YES: Néron 1950, Honda 1960.
- Later, most conjectured NO: Cassels 1966, Tate 1974, Mestre 1982, Silverman 1986, 2009, Brumer 1992, Ulmer 2002, Farmer–Gonek–Hughes 2007.

Heuristics for boundedness

- Rubin and Silverberg 2000: Equidistribution of certain lattices would imply that quadratic twists of a fixed E have rank bounded by 8 (false for some E).
- Granville $\sim$ 2006, published in Watkins–Donnelly–Elkies–Fisher–Granville–Rogers 2014: Heuristics for counting integer solutions to equations suggest that all but finitely many quadratic twists of a fixed E have rank bounded by 7.
- Watkins 2015: A variant of Granville's heuristic suggests that in the family of all elliptic curves over $\mathbb{Q}$, all but finitely many have rank ≤ 21.

We will present a different heuristic, which models ranks, Selmer groups, and Shafarevich–Tate groups simultaneously and predicts that $\operatorname{rk} E(\mathbb{Q}) \leq 21$ for all but finitely many $E \in \mathscr{E}$.

Selmer groups and Shafarevich–Tate groups

For each E, one has

$$0 \longrightarrow \frac{E(\mathbb{Q})}{nE(\mathbb{Q})} \longrightarrow \underbrace{\mathrm{Sel}_n E}_{n\text{-Selmer group}} \longrightarrow \underbrace{Ш[n]}_{\substack{n\text{-torsion of the} \\ \text{Shafarevich–Tate group}}} \longrightarrow 0.$$

In fact, the only known way to bound $\mathrm{rk}\, E(\mathbb{Q})$ is to compute Selmer groups.

Setting $n = p^e$ and taking $\varinjlim_e$ yields

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0.$$

We will model these sequences.

Model for $\mathrm{Sel}_p E$

Equip the $\mathbb{F}_p$-vector space $V_n := \mathbb{F}_p^{2n}$ with the quadratic form

$$Q(x_1, \ldots, x_n, y_1, \ldots, y_n) := x_1 y_1 + \cdots + x_n y_n.$$

Call a subspace $Z \subseteq V_n$ maximal isotropic if $Q|_Z = 0$ and $Z^\perp = Z$.

Conjecture (P.–Rains 2012)

The distribution of $\dim \mathrm{Sel}_p E$ *as* E *ranges over* $\mathscr{E}$ *equals*
$\lim_{n\to\infty}$ *of the distribution of* $\dim(Z \cap W)$
for random maximal isotropic subspaces Z, W *of* V_n.

Model for $\mathrm{Sel}_p E$, continued

Conjecture (P.–Rains 2012, copied from previous slide)

The distribution of $\dim \mathrm{Sel}_p E$ *as* E *ranges over* $\mathscr{E}$ *equals*
$\lim_{n\to\infty}$ *of the distribution of* $\dim(Z \cap W)$
for random maximal isotropic subspaces Z, W *of* V_n.

Equivalent conjecture

For each $s \geq 0$, *the density of* $\{E \in \mathscr{E} : \dim \mathrm{Sel}_p E = s\}$ *equals*

$$\prod_{j\geq 0}(1+p^{-j})^{-1}\prod_{j=1}^{s}\frac{p}{p^j-1}.$$

Reasons to believe:

- A variant for many quadratic twist families is *proved* for $p = 2$ (Heath-Brown 1994, Swinnerton-Dyer 2008, Kane 2013).
- $\mathrm{Sel}_p E$ *is* an intersection of two maximal isotropic subgroups (P.–Rains 2012).
- The conjecture is compatible with the Bhargava–Shankar theorems on average Selmer group size.

From Sel_p to Sel_{p^e} and Sel_{p^∞}

Conjecture (P.–Rains 2012, copied from earlier slide)

The distribution of $\dim \mathrm{Sel}_p E$ *as* E *ranges over* $\mathscr{E}$ *equals* $\lim_{n\to\infty}$ *of the distribution of* $\dim(Z \cap W)$ *for random maximal isotropic subspaces* Z, W *of* V_n.

Bhargava–Kane–Lenstra–P.–Rains 2015: Generalizing leads to

- a conjectural distribution for $\mathrm{Sel}_{p^e} E$;
- a conjectural distribution for the whole sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0;$$

- for each $r \geq 0$, a conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$.

Reason to believe: A variant for many quadratic twist families is *proved* for $p = 2$ (Alexander Smith).

From Sel_p to Sel_{p^e} and Sel_{p^∞}

Conjecture (P.–Rains 2012, copied from earlier slide)

The distribution of $\dim \mathrm{Sel}_p E$ *as* E *ranges over* $\mathscr{E}$ *equals* $\lim_{n\to\infty}$ *of the distribution of* $\dim(Z \cap W)$ *for random maximal isotropic subspaces* Z, W *of* V_n.

Bhargava–Kane–Lenstra–P.–Rains 2015: Generalizing leads to

- a conjectural distribution for $\mathrm{Sel}_{p^e} E$;
- a conjectural distribution for the whole sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_{p^\infty} E \longrightarrow Ш[p^\infty] \longrightarrow 0;$$

- for each $r \geq 0$, a conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$.

Reason to believe: A variant for many quadratic twist families is *proved* for $p = 2$ (Alexander Smith).

Model for $Ш[p^\infty]$

For each $r \geq 0$, the conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$ equals the distribution constructed as follows:

1. Define $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}} := \{A \in \mathrm{M}_n(\mathbb{Z}_p) : A^T = -A\}$.
2. View each $A \in \mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}} \subseteq \mathrm{M}_n(\mathbb{Z}_p)$ as a homomorphism $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$ to define $\ker A$ and $\operatorname{coker} A$.
3. Sample A from the space of matrices in $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ satisfying $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r$.
4. Take the distribution of $(\operatorname{coker} A)_{\mathrm{tors}}$.
5. Take the limit of this distribution as $n \to \infty$ through integers $\equiv r \pmod 2$.

(The distribution also equals a distribution defined by Delaunay 2001, 2007 and Delaunay–Jouhet 2014, who adapted the Cohen–Lenstra heuristics for class groups.)

Model for $Ш[p^\infty]$

For each $r \geq 0$, the conjectural distribution for $Ш[p^\infty]$ as E ranges over rank r curves in $\mathscr{E}$ equals the distribution constructed as follows:

1. Define $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}} := \{A \in \mathrm{M}_n(\mathbb{Z}_p) : A^T = -A\}$.
2. View each $A \in \mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}} \subseteq \mathrm{M}_n(\mathbb{Z}_p)$ as a homomorphism $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$ to define $\ker A$ and $\operatorname{coker} A$.
3. Sample A from the space of matrices in $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ satisfying $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r$.
4. Take the distribution of $(\operatorname{coker} A)_{\mathrm{tors}}$.
5. Take the limit of this distribution as $n \to \infty$ through integers $\equiv r \pmod 2$.

(The distribution also equals a distribution defined by Delaunay 2001, 2007 and Delaunay–Jouhet 2014, who adapted the Cohen–Lenstra heuristics for class groups.)

Modeling the rank of an elliptic curve

- Previous slide: Conditioning on $\mathrm{rk}_{\mathbb{Z}_p}(\ker A) = r$ yields the conjectural distribution of $Ш[p^\infty]$ for rank r curves.
- Simplest possible explanation for this: Sampling A from $\mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ *without* conditioning on $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ causes $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ to be distributed like the rank of an elliptic curve.

What is the distribution of $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$?

Answer: With probability 1, it is

$$\begin{cases} 0 \text{ if } n \text{ is even;} \\ 1 \text{ if } n \text{ is odd.} \end{cases}$$

(It is only on a lower-dimensional locus that $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ is larger.)

This is compatible with the "Goldfeld conjecture" that rank is

$$\begin{cases} 0 & \text{for 50\% of elliptic curves;} \\ 1 & \text{for 50\% of elliptic curves;} \\ \geq 2 & \text{for 0\% of elliptic curves.} \end{cases}$$

Modeling the rank of an elliptic curve, continued

- Previous model: $\mathrm{rk}_{\mathbb{Z}_p}(\ker A)$ for $A \in \mathrm{M}_n(\mathbb{Z}_p)_{\mathrm{alt}}$ models rank.
- Refined model: $\mathrm{rk}_{\mathbb{Z}}(\ker A)$ for $A \in \mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\leq X}$ models rank, where $\mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\leq X}$ is the set of matrices in $\mathrm{M}_n(\mathbb{Z})_{\mathrm{alt}}$ with entries bounded by a number X depending on the height H of the elliptic curve being modeled, with $X \to \infty$ as $H \to \infty$.

Advantage of this refined model:

For elliptic curves of a given height H,

- the model predicts a potentially positive but diminishing probability of each rank ≥ 2, and
- we can quantify the rate at which this probability tends to 0 as $H \to \infty$ in order to count curves in $\mathscr{E}_{\leq H}$ having each given rank.

In fact, we let n grow with H as well.

THE model

To model an elliptic curve E of height H, we do the following, using growing functions $\eta(H)$ and $X(H)$ to be specified later:

1. Choose n to be an integer of size about $\eta(H)$ of random parity.
2. Choose random $A_E \in \mathrm{M}_n(\mathbb{Z})_{\mathrm{alt},\leq X(H)}$, independently for each E.
3. Define random variables

$$Ш'_E := (\operatorname{coker} A)_{\mathrm{tors}} \quad \text{and} \quad \mathrm{rk}'_E := \mathrm{rk}_{\mathbb{Z}}(\ker A).$$

These are supposed to model $Ш(E)$ and $\mathrm{rk}\, E(\mathbb{Q})$, respectively.

The functions $\eta(H)$ and $X(H)$ are chosen so that

$$X(H)^{\eta(H)} = H^{1/12+o(1)};$$

it turns out that this ensures that for rank 0 curves, the averages of $Ш'_E$ and $Ш(E)$ match (conditionally on standard conjectures).

Consequences of the model

Theorem (Park–P.–Voight–Wood)

The following hold with probability 1*:*

$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E = 0\} = H^{20/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E = 1\} = H^{20/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 2\} = H^{19/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 3\} = H^{18/24+o(1)}$$
$$\vdots$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 20\} = H^{1/24+o(1)}$$
$$\#\{E \in \mathscr{E}_{\leq H} : \mathrm{rk}'_E \geq 21\} \leq H^{o(1)},$$

$\#\{E \in \mathscr{E} : \mathrm{rk}'_E > 21\}$ is finite.

For comparison: Elkies found

- infinitely many elliptic curves of rank at least 19, and
- one elliptic curve of rank at least 28.

Elliptic curves with prescribed torsion subgroup

torsion subgroup	# curves	our rank bound	known example
trivial	$H^{5/6}$	21	19
$\mathbb{Z}/2\mathbb{Z}$	$H^{1/2}$	13	11
$\mathbb{Z}/3\mathbb{Z}$	$H^{1/3}$	9	7
$\mathbb{Z}/4\mathbb{Z}$	$H^{1/4}$	7	6
$\mathbb{Z}/5\mathbb{Z}$	$H^{1/6}$	5	4
$\mathbb{Z}/6\mathbb{Z}$	$H^{1/6}$	5	5
$\mathbb{Z}/7\mathbb{Z}$	$H^{1/12}$	3	2
$\mathbb{Z}/8\mathbb{Z}$	$H^{1/12}$	3	3
$\mathbb{Z}/9\mathbb{Z}$	$H^{1/18}$	2	1
$\mathbb{Z}/10\mathbb{Z}$	$H^{1/18}$	2	1
$\mathbb{Z}/12\mathbb{Z}$	$H^{1/24}$	2	1
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$H^{1/3}$	9	8
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$H^{1/6}$	5	5
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$H^{1/12}$	3	3
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$H^{1/24}$	2	1

Elliptic curves over global fields: heuristics

- K: a global field
- $\mathscr{E}_K$: a set of representatives for the isomorphism classes of elliptic curves over K
- $B_K := \limsup_{E \in \mathscr{E}_K} \operatorname{rk} E(K)$.

Example

Our heuristic predicts $20 \leq B_{\mathbb{Q}} \leq 21$.

A naive adaptation of our heuristic would suggest that

$$20 \leq B_K \leq 21 \text{ for every global field } K.$$

Question

How does this compare with reality?

Not well...

Elliptic curves over global fields: reality

Theorem (Tate–Shafarevich 1967, Ulmer 2002)

If K is a global function field, then $B_K = \infty$.

Even for number fields, B_K can be arbitrarily large
(but maybe still always finite):

Theorem (Park–P.–Voight–Wood)

There exist number fields K of arbitrarily high degree such that $B_K \geq [K : \mathbb{Q}]$.

Number fields for which B_K is large include

- number fields in anticyclotomic towers and
- certain multiquadratic fields.

Elliptic curves over global fields: reconciliation

Question

How do we explain the differences between our heuristic and reality?

The elliptic curves of high rank used to prove that B_K is large for some K are special in that they are definable over a proper subfield of K. Exclude them!

- $\mathscr{E}_K^\circ$: the set of $E \in \mathscr{E}_K$ such that
  E is not a base change of a curve from a proper subfield.
- $B_K^\circ := \limsup_{E \in \mathscr{E}_K^\circ} \operatorname{rk} E(K)$.

Speculation

It is possible that $B_K^\circ < \infty$ for every global field K.

On the other hand, it is not true that $B_K^\circ \leq 21$ for all number fields: Shioda's rank 68 elliptic curve $y^2 = x^3 + t^{360} + 1$ over $\mathbb{C}(t)$ specializes to show that $B_K^\circ \geq 68$ for many number fields K.

Abelian varieties

Question

For abelian varieties A over number fields K, is there a bound on $\mathrm{rk}\, A(K)$ *depending only on* $\dim A$ *and* $[K : \mathbb{Q}]$*?*

- Fix g. By restriction of scalars and Zarhin's trick, one reduces to considering one algebraic family $\mathcal{F}_g$ of principally polarized abelian varieties over $\mathbb{Q}$.
- Define the height of $A \in \mathcal{F}_g$ in terms of coefficients of defining polynomials.
- The number of abelian varieties in $\mathcal{F}_g$ of height $\leq H$ is bounded by a polynomial in H.
- If, as for elliptic curves, there is a model involving a pseudo-rank rk'_A such that $\mathrm{Prob}(\mathrm{rk}'_A \geq r)$ gets divided by at least a fixed fractional power of H each time r is incremented by 1, then the pseudo-ranks are bounded with probability 1.
- Thus maybe actual ranks are bounded too.

Guess: YES!

Summary

- Heuristics for Selmer groups led to a model for the complete package consisting of ranks, Selmer groups, and Shafarevich–Tate groups.
- Many aspects of the model are supported by theorems.
- In the model, the pseudo-ranks of all but finitely many elliptic curves over $\mathbb{Q}$ are bounded by 21.
- This suggests that $\operatorname{rk} E(\mathbb{Q})$ is uniformly bounded as E varies.

Also,

- Similar heuristics may apply to elliptic curves over global fields, after excluding curves definable over proper subfields.
- Similar heuristics may apply to abelian varieties of fixed dimension over a fixed number field.